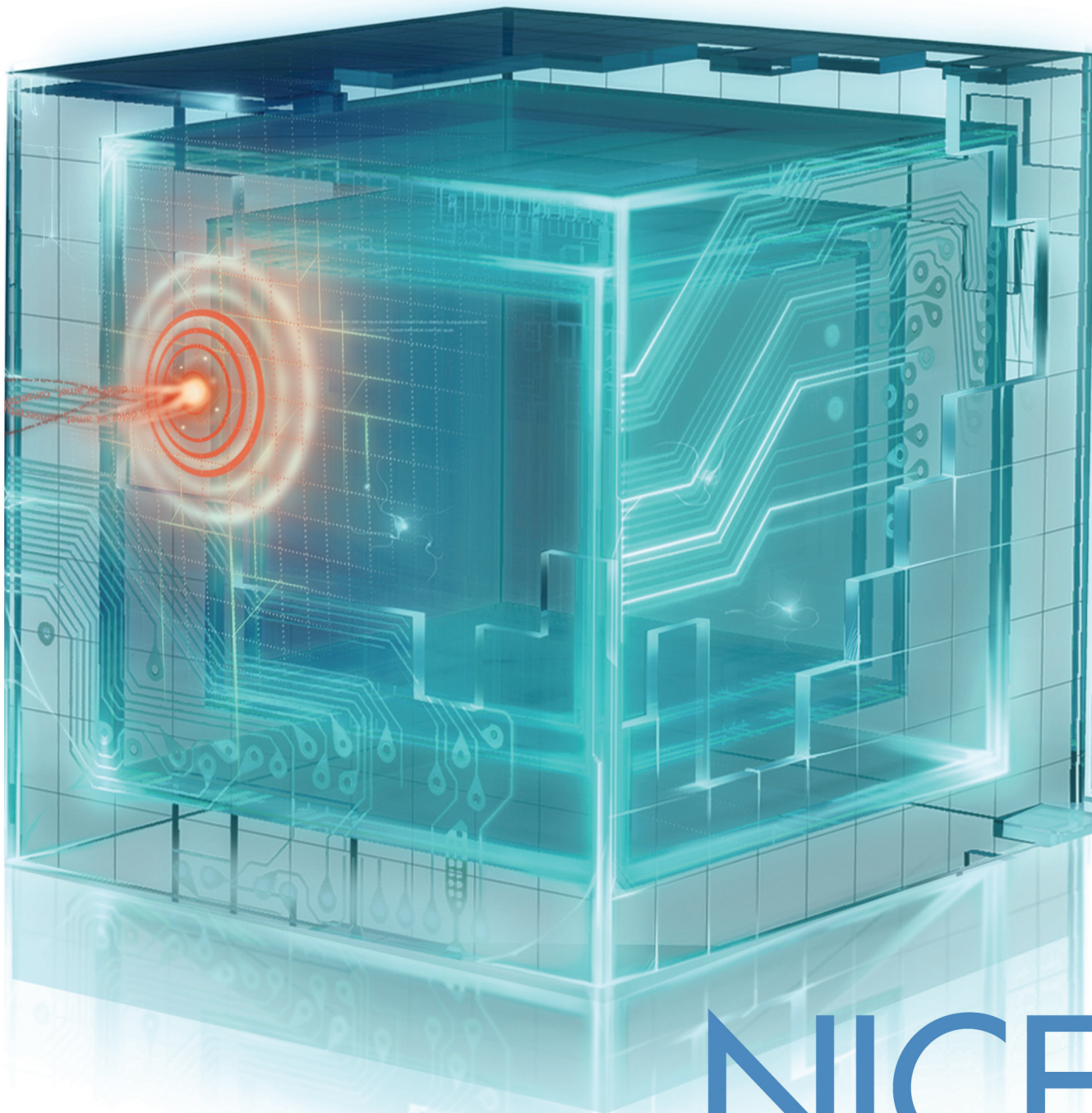


CYBERSECURITY
WORKFORCE
FRAMEWORK



NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

INTRODUCTION

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Two Executive Branch initiatives, in 2008 and 2010, founded the NICE. It seeks to encourage and build cybersecurity awareness and competence across the nation and to develop an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of cyber threats.

Today, there is little consistency in how cybersecurity work is defined or described throughout the Federal Government and the nation. The absence of a common language to discuss and understand the work and skill requirements of cybersecurity professionals hinders our nation's ability to baseline capabilities, identify skill gaps, develop cybersecurity talent in the current workforce, and prepare the pipeline of future talent. Consequently, establishing and using a common lexicon and taxonomy for cybersecurity work and workers is not merely desirable, but vital to the nation's cybersecurity.

To this end, this document, *The NICE Cybersecurity Workforce Framework*, puts forth a working taxonomy and common lexicon that can be overlaid onto any organization's existing occupational structure. It has been developed largely with input from the Federal Government, but that is not sufficient; we need to ensure that this framework can be adopted and used across the nation in both the public and private sectors. Moreover, the framework should address emerging work requirements to help ensure the nation has the skills to meet them. Therefore, we seek to refine this framework with input from every sector of our nation's cybersecurity stakeholders, including academia, professional, and non-profit organizations, and private industry. Much as other professions such as medicine and law, have codified their specialties, it is now time to forge a common set of definitions for the cybersecurity workforce.

This framework organizes cybersecurity into seven high-level categories, each comprising several specialty areas. This organizing structure is based on extensive job analyses and groups together work and workers that share common major functions, regardless of actual job titles or other occupational terms. As the job analysis information regarding these specialty areas is extensive, only the framework is published here. Additional details regarding each specialty area, as well as more information about the framework in general, is available online (please see the end of this booklet). Therefore, the goal of this document is simply to introduce you to *The NICE Cybersecurity Workforce Framework* and to seek your help to ensure that it is a robust foundation for creating and sustaining a world-class cybersecurity workforce for America.

SECURELY PROVISION

Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development.

Information Assurance Compliance

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.

(Example job titles: Accreditor; Auditor; Authorizing Official Designated Representative; Certification Agent; Certifying Official; Compliance Manager; Designated Accrediting Authority; IA Compliance Analyst/Manager; IA Manager; IA Officer; Portfolio Manager; Risk/Vulnerability Analyst; Security Control Assessor; Validator)

Software Engineering

Develops, creates, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

(Example job titles: Analyst Programmer; Computer Programmer; Configuration Manager; IA Engineer; A Software Developer; IA Software Engineer; R&D Engineer; Secure Software Engineer; Security Engineer; Software Developer; Systems Analyst; Web Application Developer)

Enterprise Architecture

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

(Example job titles: IA Architect; Information Security Architect; Information Systems Security Engineer; Network Security Analyst; R&D Engineer; Security Architect; Security Engineer; Security Solutions Architect; Systems Engineer; Systems Security Analyst)

Technology Demonstration

Conducts technology assessment and integration processes; provides and supports a prototype capability and evaluates its utility.

(Example job titles: Capabilities and Development Specialist; R&D Engineer)

Systems Requirements Planning

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

(Example job titles: Business Analyst; Business Process Analyst; Computer Systems Analyst; Contracting Officer; Contracting Officer's Technical Representative (COTR); Human Factors Engineer; Requirements Analyst; Solutions Architect; Systems Consultant; Systems Engineer)

Test and Evaluation

Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

(Example job titles: Application Security Tester; Information Systems Security Engineer; Quality Assurance Tester; R&D Engineer; Systems Engineer; Testing and Evaluation Specialist)

Systems Development

Works on the development phases of the systems development lifecycle.

(Example job titles: IA Developer; IA Engineer; Information Systems Security Engineer; Program Developer; Security Engineer; Systems Engineer)

OPERATE AND MAINTAIN

Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

Data Administration

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

(Example job titles: Content Staging Specialist; Data Architect; Data Manager; Data Warehouse Specialist; Database Administrator; Database Developer; Information Dissemination Manager)

Information System Security Management

Oversees the information assurance program of an information system inside or outside the network environment; may include procurement duties (e.g., ISSO).

(Example job titles: IA Manager; Information Assurance Security Officer; Information Systems Security Officer (ISSO); Information Security Program Manager)

Knowledge Management

Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

(Example job titles: Business Analyst; Business Intelligence Manager; Content Administrator; Document Steward; Freedom of Information Act Official; Information Manager; Information Owner; Information Resources Manager)

Customer Service and Technical Support

Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

(Example job titles: Computer Support Specialist; Customer Support; Help Desk Representative; Service Desk Operator; Systems Administrator; Technical Support Specialist)

Network Services

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

(Example job titles: Cabling Technician; Converged Network Engineer; Network Administrator; Network Analyst/Designer/Engineer; Network Systems and Data Communications Analyst; Telecommunications Engineer)

System Administration

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control/ passwords/ account creation and administration.

(Example job titles: LAN Administrator; Platform Specialist; Security Administrator; Server Administrator; System Operations Personnel; Systems Administrator; Website Administrator)

Systems Security Analysis

Conducts the integration/testing, operations, and maintenance of systems security.

(Example job titles: IA Operational Engineer; IA Security Officer; Information Security Analyst/Administrator/Manager; Information Systems Security Engineer; Platform Specialist; Security Administrator; Security Analyst; Security Control Assessor)

PROTECT AND DEFEND

Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.

Computer Network Defense

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

(Example job titles: CND Analyst (Cryptologic); Cyber Security Intelligence Analyst; Focused Operations Analyst; Incident Analyst; Network Defense Technician; Security Analyst; Security Operator; Sensor Analyst)

Incident Response

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

(Example job titles: Computer Crime Investigator; Incident Handler; Incident Responder; Intrusion Analyst)

Computer Network Defense Infrastructure Support

Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

(Example job titles: IDS Administrator; IDS Engineer; IDS Technician; Information Systems Security Engineer; Network Administrator; Network Analyst; Network Security Engineer/Specialist; Security Analyst; Security Engineer; Security Specialist)

Security Program Management

Manages relevant security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).

(Example job titles: Chief Information Security Officer (CISO); Common Control Provider; Enterprise Security Officer; Facility Security Officer; IT Director; Principal Security Architect; Risk Executive; Senior Agency Information Security Officer)

Vulnerability Assessment and Management

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

(Example job titles: Blue Team Technician; Close Access Technician; CND Auditor; Compliance Manager; Ethical Hacker; Governance Manager; Internal Enterprise Auditor; Penetration Tester; Red Team Technician; Reverse Engineer; Risk/Vulnerability Analyst/Manager)

INVESTIGATE

Specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.

Investigation

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, countersurveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

(Example job titles: Computer Crime Investigator; Special Agent)

Digital Forensics

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence, or law enforcement investigations.

(Example job titles: Computer Network Defense Forensic Analyst; Digital Forensic Examiner; Digital Media Collector; Forensic Analyst; Forensic Analyst (Cryptologic); Forensic Technician; Network Forensic Examiner)

OPERATE AND COLLECT

Specialty areas responsible for the highly specialized collection of cybersecurity information that may be used to develop intelligence.

Collection Operations

Executes collection using appropriate collection strategies and within the priorities established through the collection management process.

Cyber Operations Planning

Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

Cyber Operations

Uses automated tools to manage, monitor, and/or execute large-scale cyber operations in response to national and tactical requirements.

ANALYZE

Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Cyber Threat Analysis

Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Exploitation Analysis

Analyzes collected information to identify vulnerabilities and potential for exploitation.

All Source Intelligence

Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

Targets

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

SUPPORT

Specialty areas providing support so that others may effectively conduct their cybersecurity work.

Legal Advice and Advocacy

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

(Example job titles: Legal Advisor/SJA)

Strategic Planning and Policy Development

Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

(Example job titles: Chief Information Officer (CIO); Command IO; Information Security Policy Analyst; Information Security Policy Manager; Policy Writer and Strategist)

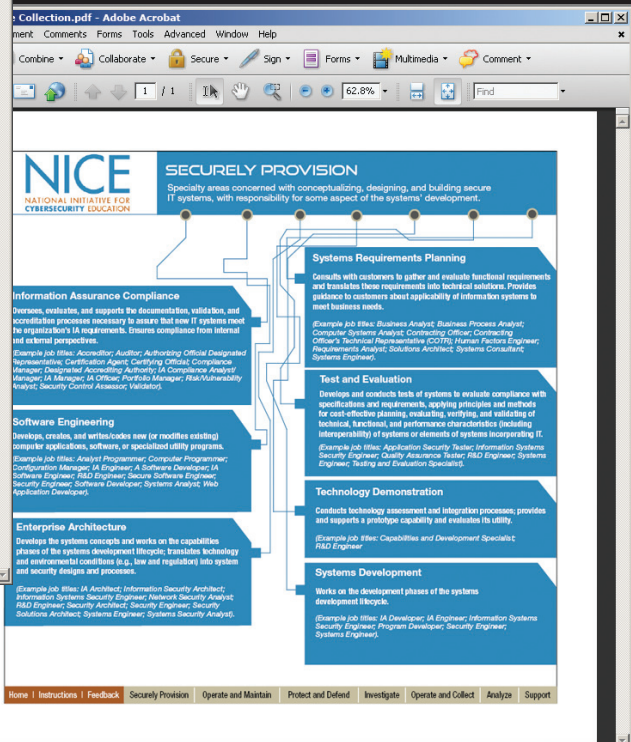
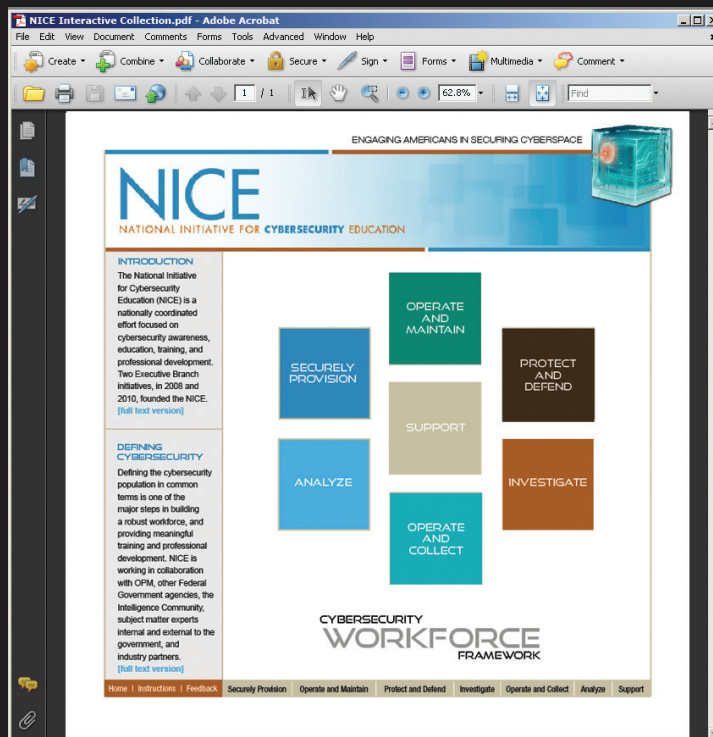
Education and Training

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

(Example job titles: Cyber Trainer; Information Security Trainer; Security Training Coordinator)

LEARN MORE

Online you will find links to a more in-depth and interactive document that dives into each specialty area providing example job titles; tasks; and knowledge, skills, and abilities (KSAs) associated with each specialty area. The following provides a sample of the kind of information you can find online:



For detailed job descriptions go to:
<http://csrc.nist.gov/nice/framework>

GET INVOLVED

This online document also contains additional background information and instructions for providing feedback.

Please use the QR code or URL below for online access:



<http://csrc.nist.gov/nice/framework/>

NICE is committed to developing a comprehensive and meaningful framework and lexicon that effectively defines our current cybersecurity population. Your feedback and expertise are invaluable to this process. Below are a few questions you may find helpful in formulating your comments.

- 1. Are the specialty areas appropriately grouped within each major category?***
- 2. Is there a specialty area you believe is not represented?***
- 3. Is there a specialty area that should be deleted?***

In the full document, accessible through the URL above, you will also have an opportunity to review and provide feedback on the more detailed information within each specialty area (i.e., tasks and skills necessary to perform the work).

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION
<http://csrc.nist.gov/nice>

SEPTEMBER 2011